

о том, что наиболее устойчивой по отношению к помехам является система с пропорционально-интегрирующим фильтром в цепи обратной связи, а наименее устойчивой является система без фильтра в цепи обратной связи.

Таким образом, на основании результатов исследуемых методов система ФАПЧ с пропорционально-интегрирующим фильтром в петле обратной связи является наиболее помехоустойчивой. В пределах полосы захвата при значительных значениях мощности шума вероятность срыва слежения у данного вида системы низка.

Список литературы

1. Шахгильдян В. В., Ляховкин А. А. Система фазовой автоподстройки частоты. М. : Связь, 1972. 447 с.
2. Обрезков Г. В., Разевиг В. Д. Методы анализа срыва слежения. М. : Сов. радио, 1972. 240 с.
3. Астрецов Д. В. Следящие радиосистемы : учеб. электрон. издание. Екатеринбург, УрФУ, 2010.

УДК 004.056

Н. А. Остапенко, А. П. Ярьсько

Научный руководитель: канд. тех. наук, доц. А. Н. Соколов
Южно-Уральский государственный университет, Челябинск

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧЕК ПО КАНАЛУ АКУСТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Аннотация. В статье проведен сравнительный анализ актуальных средств защиты информации от утечек по каналу акустоэлектрических преобразований, показана эффективность каждого метода, его достоинства и недостатки. Методика построения защиты условно поделена на два этапа (специальные исследования технических средств и применение средств защиты). Сделан вывод о целесообразности использования рассмотренных технических решений.

Ключевые слова: информационная безопасность; защита информации; средства защиты информации; специальные исследования; акустоэлектрические преобразования; генераторы шума.

Утечка информации по каналу акустоэлектрических преобразований — одна из важнейших проблем технической защиты информации. Акустоэлектрическим эффектом обладают многие элементы электронных технических

средств обработки информации и вспомогательных технических средств. Прежде всего это моточные изделия, в которых в соответствии с законом электромагнитной индукции, открытым Фарадеем, наводится ЭДС при движении проводников в магнитном поле под действием энергии звуковой волны. Магнитное поле всегда присутствует в ферромагнитных сердечниках за счет остаточной индукции. Построение защиты от такой утечки информации можно условно разделить на два этапа: специальные исследования и средства защиты.

Специальные исследования технических средств на предмет отсутствия акустоэлектрических преобразований проводится для установления нерегламентированных возможностей технических средств преобразовывать акустический сигнал в электрический и передачу этого сигнала по линиям коммуникаций. Это лицензируемый вид деятельности в Российской Федерации. Организации-лицензиаты в специальных лабораториях проводят исследования технических средств на наличие в них признаков акустоэлектрических преобразования и выдают заказчику заключение по результатам проведенных работ. Несмотря на то, что данные исследования проводятся в полном объеме и достаточно точно определяют наличие акустоэлектрических преобразований, они не могут дать гарантии полного отсутствия канала утечки в техническом средстве в виду несовершенства некоторых методических указаний и постоянном совершенствовании средств разведки. Помимо этого, данный этап поможет только в том случае, если в техническом средстве отсутствует данный канал утечки информации.

Средства защиты информации от утечки по каналам акустоэлектрических преобразований можно условно разделить на два вида: активные и пассивные.

К активным видам защиты относятся генераторы шума, которые будут зашумлять линию, выходящую за пределы контролируемой зоны во время проведения переговоров. Недостатком данного метода защиты является его дороговизна, по сравнению с пассивными средствами защиты, и невозможность удостовериться в работоспособности самого устройства защиты. Также помеха может быть отфильтрована злоумышленником, поэтому данный способ защиты является не самым надежным.

Активным способом защиты можно назвать и уничтожение средств прослушивания или «выжигание». При использовании такого способа в линию подается высоковольтные импульсы (до 1500 вольт), приводящие к выходу из строя технических средств злоумышленника. Данный способ является как самым опасным, так и самым малоэффективным. Опасен он тем, что во время процесса «выжигания» к линии может быть подключено другое оконечное устройство, которое будет выведено из строя. А его малая эффективность вытекает из того, что злоумышленник может подключиться к линии уже во время проведения переговоров, и его техника останется цела. Помимо этого, существ-

вует технические средства, с помощью которых можно извлекать информативные сигналы из линии, не имея к ней прямого гальванического подключения, а только находясь рядом с ней.

К пассивным средствам защиты линий, выходящих за пределы контролируемой зоны можно отнести ограничители сигналов малой амплитуды, которые позволяют практически полностью ограничить прохождение полезных сигналов в линию. Недостатком способа защиты ограничителями можно отнести его незначительное влияние на линию, к которой он подключен, ведь, помимо информативных акустических сигналов, он также может отфильтровать сигналы, необходимые для работы технического средства, установленного в помещении.

Размыкатели, как понятно из названия, размыкают линию, и злоумышленник уже не сможет получить информацию от устройства, которое находится в помещении. Они могут быть выполнены как в виде простого ключа, так и автоматического прибора, который отключает аппарат от линии при положенной трубке. Такой способ защиты является самым надежным и требующий дополнительных средств защиты только для комфортного исполнения. Но и у него есть свои недостатки, например, невозможность использования технических средств в момент проведения переговоров.

Исходя из приведенных способов защиты, можно сделать вывод, что, говоря о полной защите помещения от канала утечки акустоэлектрических преобразований, мы можем говорить лишь об отключении технических средств от линий, выходящих за пределы контролируемой зоны. Решить данную проблему может расширение границ контролируемой зоны и невозможность подключения к таким линиям злоумышленника, а также отказ от технических средств в помещениях для проведения переговоров.

УДК 004.056.4

Д. А. Паршин, А. П. Ярьско, Н. А. Остапенко

Научный руководитель: канд. тех. наук, доц. А. Н. Соколов
Южно-Уральский государственный университет, Челябинск

ЗАЩИТА USB-FLASH-НОСИТЕЛЕЙ ОТ УТЕЧЕК ИНФОРМАЦИИ ПО КАНАЛУ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

Аннотация. При хранении, обработке и передачи информации на USB-flash-носителе образуются побочные электромагнитные излучения (ПЭМИ), несущие сигнал на нечетных гармониках, затухая при возрастании, согласно теореме Фурье. Его можно перекрыть с помощью средства активного зашумления, которое генери-